



CARING LESS.

De-humanizing Human Vulnerability Assessment



LAURA BELL

FOUNDER AND LEAD CONSULTANT - SAFESTACK

@lady_nerd , laura@safestack.io

<http://safestack.io>

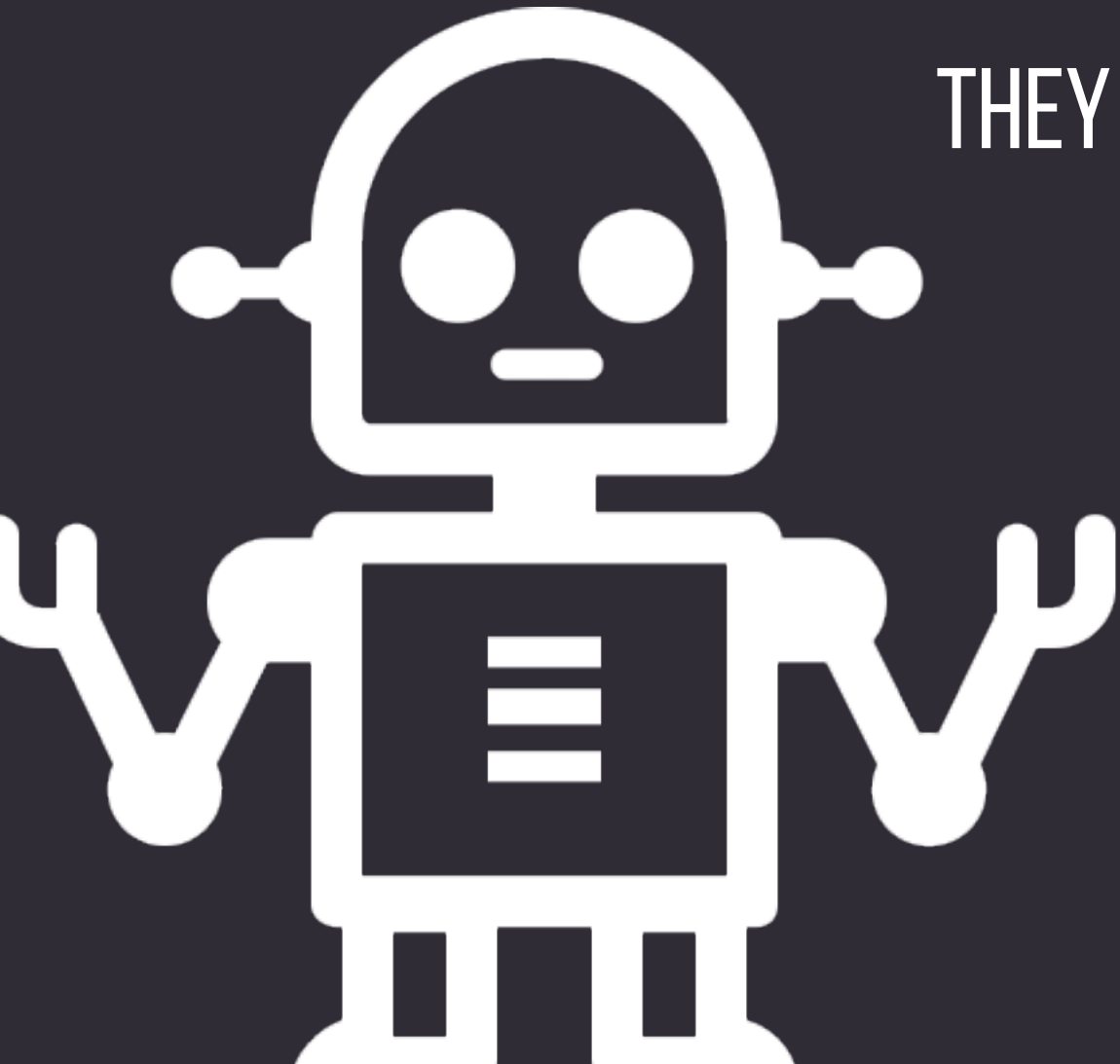


People are a problem. We are tangled balls of emotional detritus that masquerades as a trusted member of society. Underneath this lacquered veneer of respectability however writhes a tiny pink squishy ball of vulnerability - the root of all evil, well the root of security issues anyway. Let me tell you a story, let me bend your brain and make you feel uncomfortable. I want to show you why we are all our own worst enemies, why we should never ever be trusted and security people are the worst of them all.

WE ARE COMFORTABLE WHEN WE TALK ABOUT TECHNICAL
VULNERABILITY

WE DO NOT EMPATHISE OR SYMPATHISE WITH MACHINES

THEY ARE TANGIBLE, INANIMATE OBJECTS.



TECHNOLOGY IS ONLY PART OF THE SECURITY PICTURE



TECHNOLOGY



PEOPLE



PROCESS

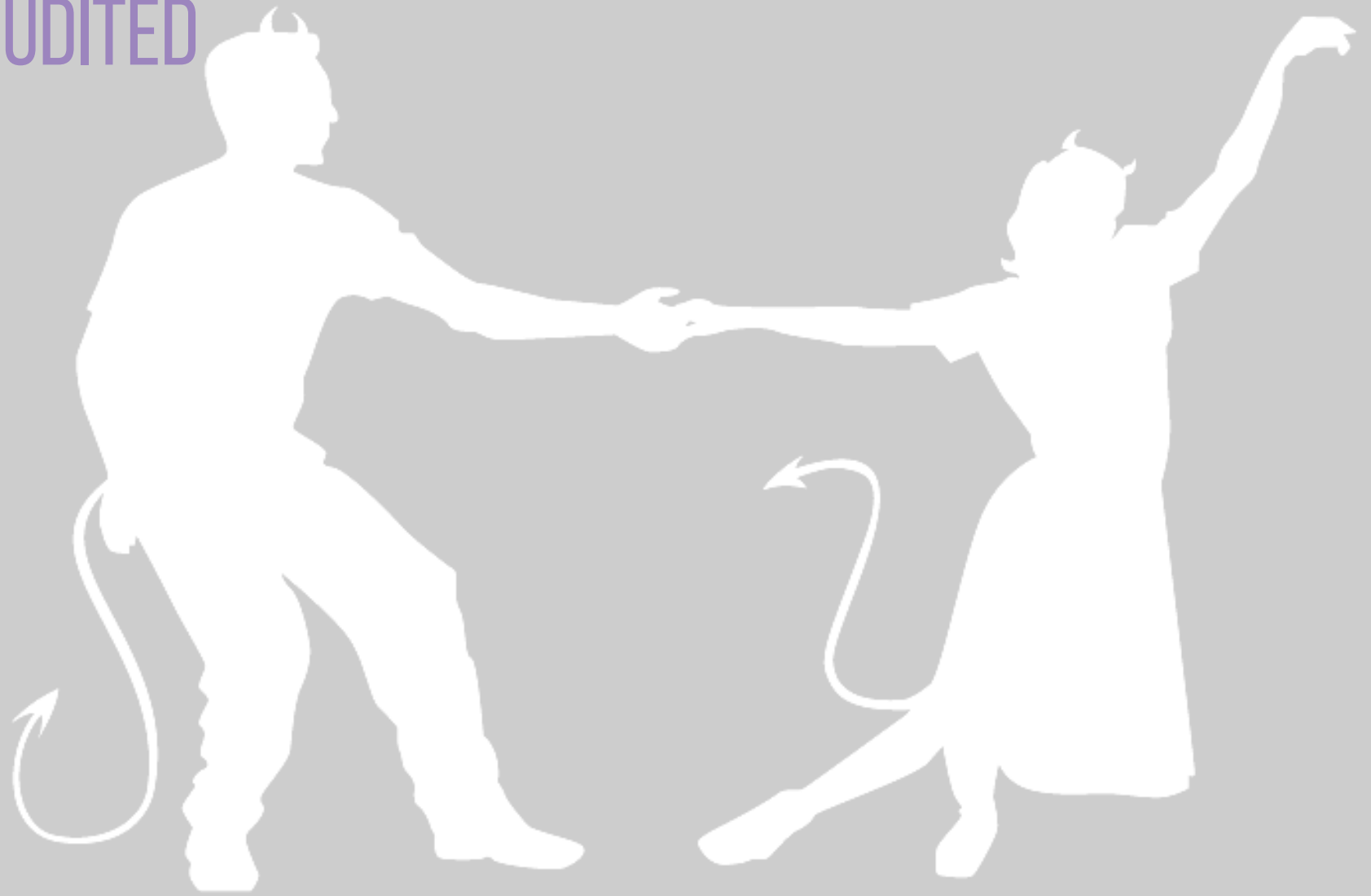
TECHNICAL SYSTEMS ARE:

REVIEWED

SCANNED

PENETRATION TESTED

PROCESSES ARE AUDITED





WHAT ABOUT PEOPLE?

IN SHORT, WE ARE FAILING

HOW DO WE MEASURE
VULNERABILITY IN PEOPLE?

SHORT ANSWER (SPOILER)

WE DON'T

AND RELATED TO THIS

HOW DO WE STRUCTURE AND PLAN HOW TO DEFEND THEM?

WE WATCH VIDEO TRAINING OR E-LEARNING

WE TICK BOXES

WE MAKE POSTERS

WE SHAME THE HUMAN VICTIMS OF HUMAN SECURITY ATTACKS*

*WHILE SECRETLY DOING THE EXACT SAME THINGS

THIS IS NOT HOW PEOPLE LEARN

JUST GO ASK THE EDUCATION AND PSYCHOLOGY COMMUNITIES

**WE LET CHILDREN FALL SO THAT THEY CAN
LEARN TO STAND**

REINFORCING BEHAVIOURS LEAD TO POSITIVE CHANGE

WE DON'T GIVE PEOPLE OPPORTUNITIES TO
FAIL SAFELY BEFORE AN ACTUAL ATTACK

WHY DON'T WE ACTIVELY ASSESS AND TEST
OUR HUMAN SECURITY RISK?

WE DON'T TEST BECAUSE IT'S TOO EASY

PEOPLE CAN'T BE TAUGHT

PEOPLE ARE LAZY

PEOPLE ARE STUPID

s/people/we/g

WE DON'T TEST

BECAUSE IT MAKES US FEEL UNCOMFORTABLE

BECAUSE WE DON'T WANT PEOPLE TO GET FIRED

BECAUSE IT'S HARD

BECAUSE WE DON'T KNOW HOW TO FIX IT

BECAUSE WE DON'T WANT PEOPLE TO GET HURT

AND FOR THE LAST TIME
MILLION DOLLAR
BORDER SECURITY
DEVICES...

WILL. NOT. SAVE. YOU

IS IT BETTER TO AVOID TESTING THE
VULNERABILITIES IN OUR PEOPLE SO THEY DON'T
GET HURT?

IS IT BETTER TO SAFELY TEST AND UNDERSTAND
THESE VULNERABILITIES SO THAT OUR PEOPLE CAN
GET STRONGER, LEARN AND BECOME MORE
RESILIENT?

CAN WE ASSESS HUMAN VULNERABILITY
WITHOUT VICTIMIZING THE PEOPLE WE
ASSESS?

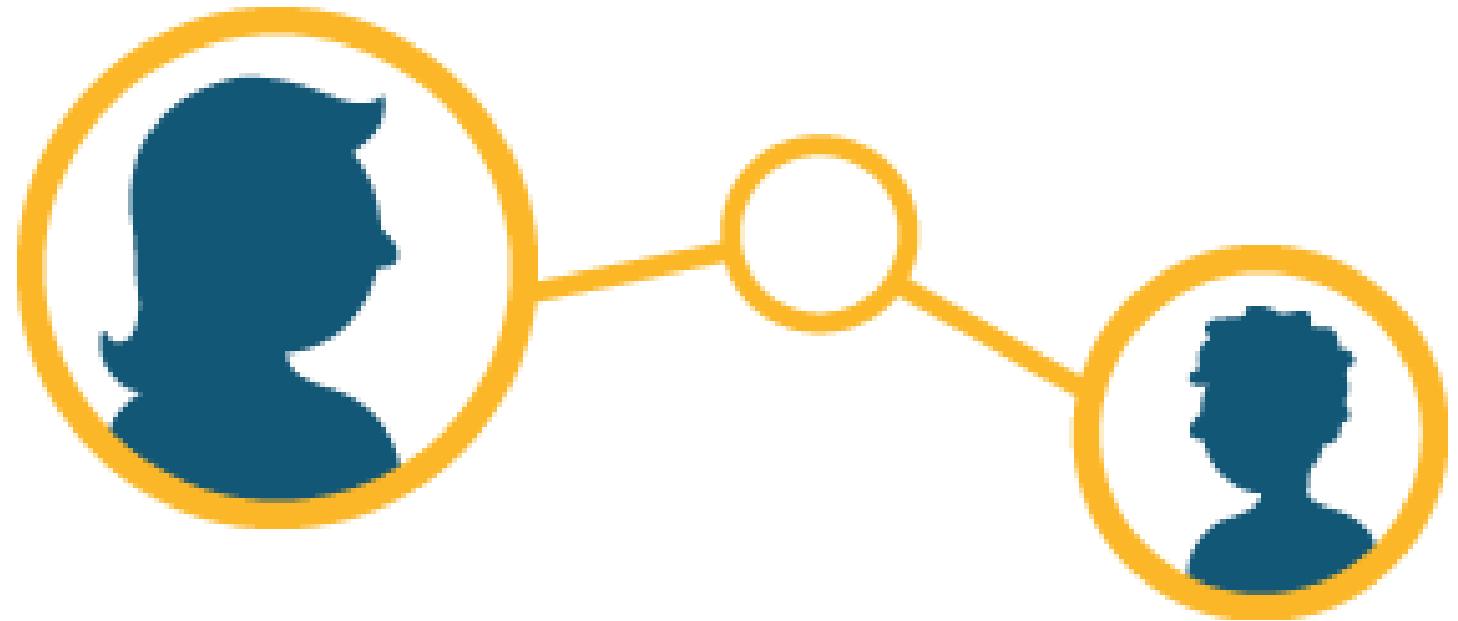
YES

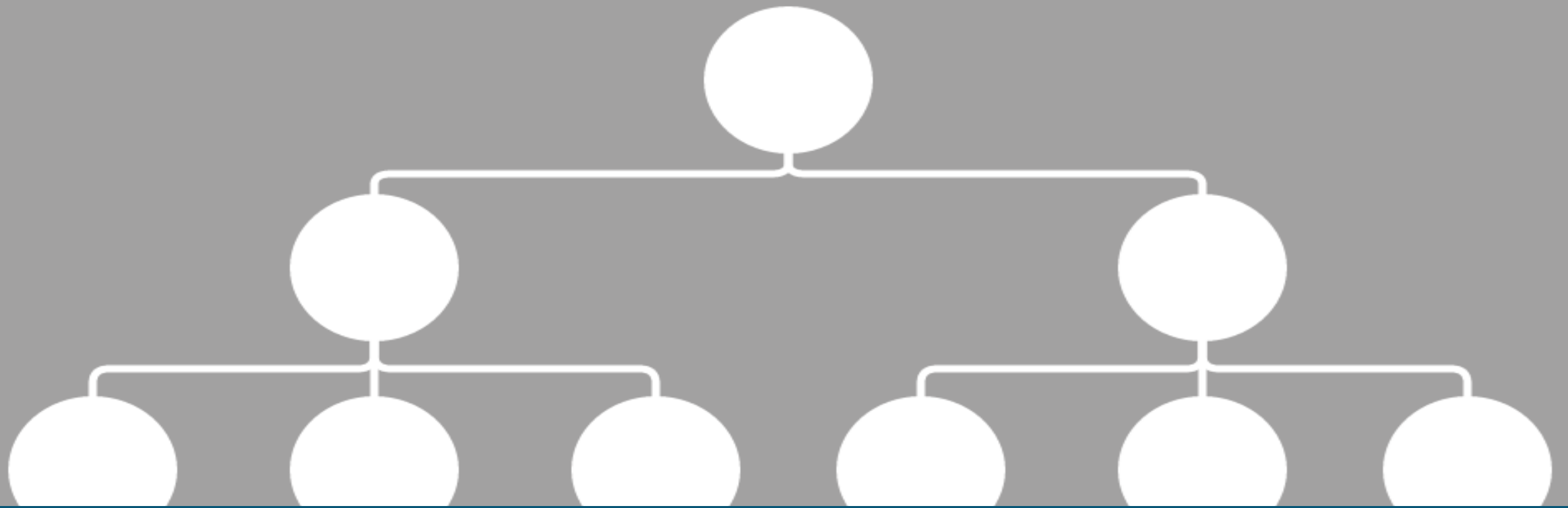
LET ME SHOW YOU HOW

AVA
FIRST GENERATION
PROOF OF CONCEPT
3- PHASE
AUTOMATED
HUMAN VULNERABILITY
SCANNER



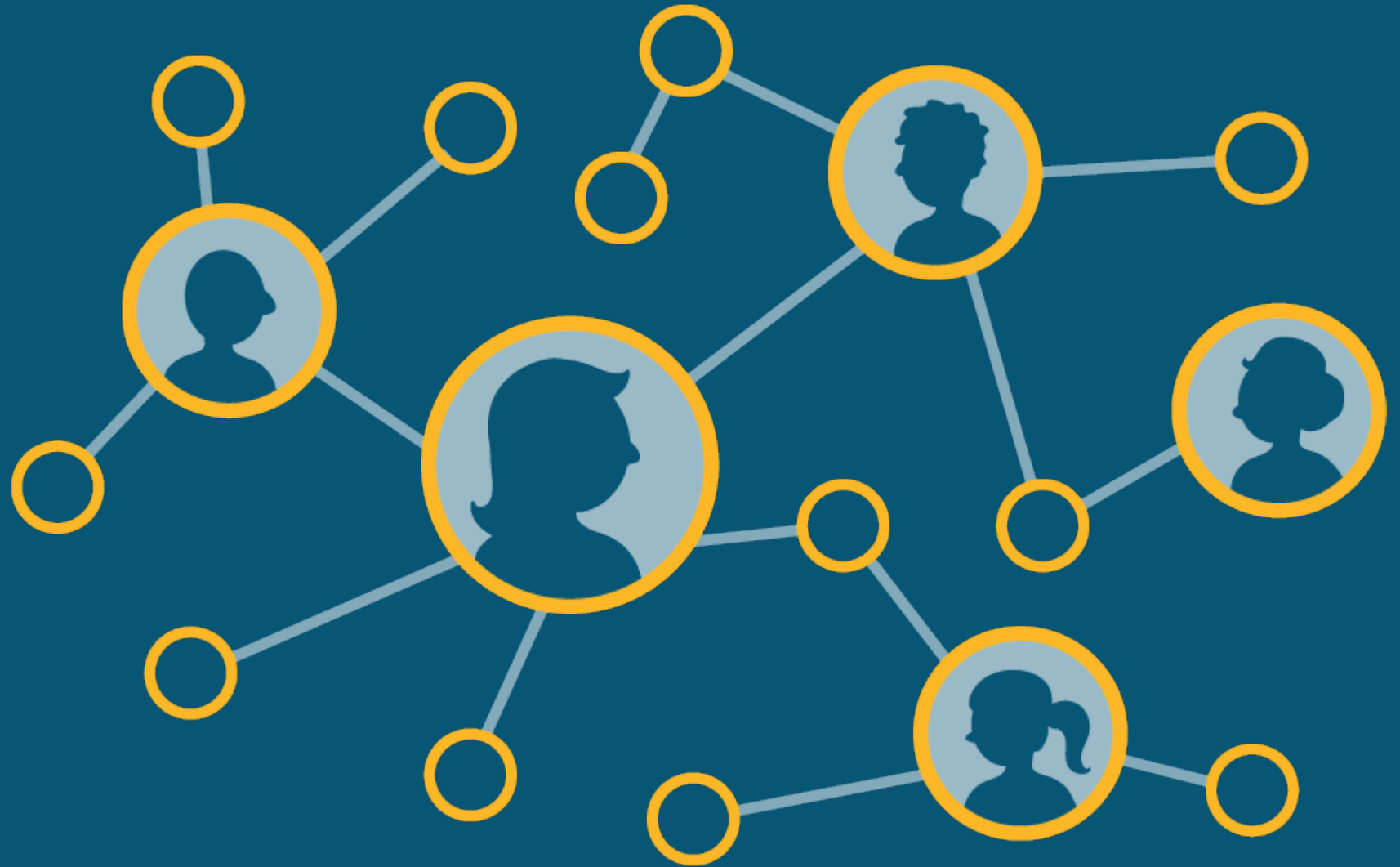
PHASE 1 **KNOW**





WE DON'T KNOW WHAT OUR ORGANISATIONS LOOK LIKE

HUMAN
SECURITY
RISK IS
MAGNIFIED
BY
CONNECTION



ACTIVE DIRECTORY

TWITTER

LINKEDIN

FACEBOOK

EMAIL PROVIDERS



PEOPLE

IDENTIFIERS

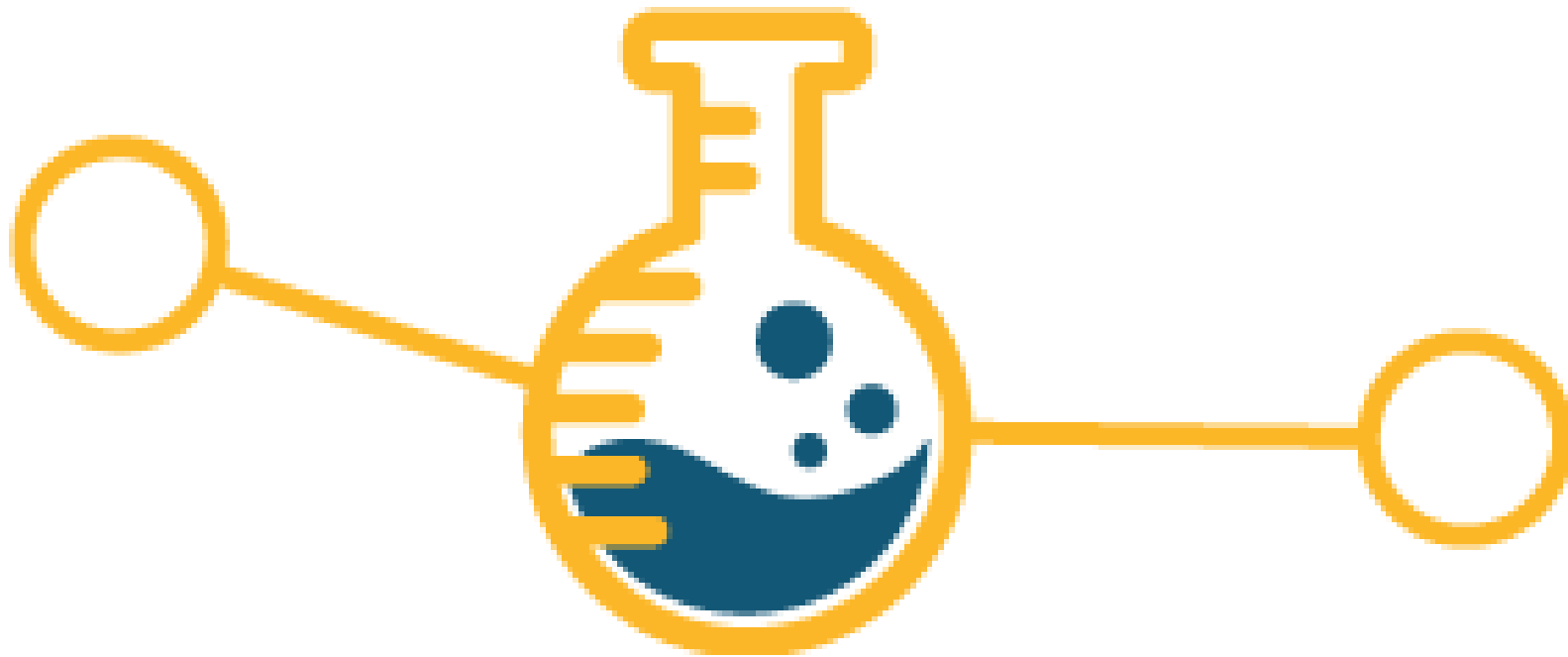
GROUPS

RELATIONSHIPS

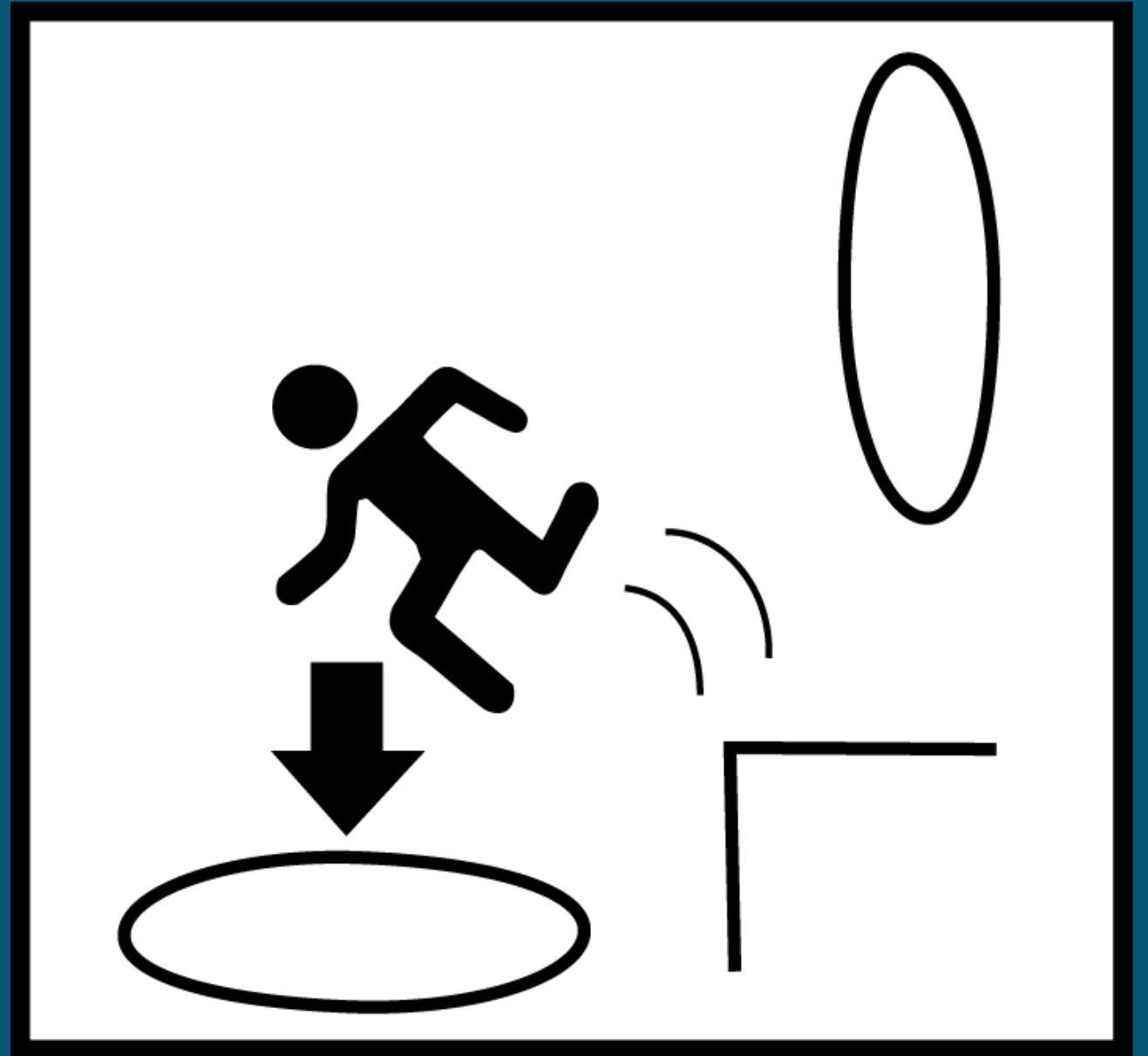
DATA

FRIENDS	LAST LOGIN	LOCATION
CONTACTS	TRAFFIC RATE	TIME STAMPS
FREQUENCY	PW EXPIRES?	SENDER
ALIASES	DISABLED?	RECEIVER
PROFILES	INFLUENCE	USER AGENT

PHASE 2 TEST



THREAT INJECTION AND BEHAVIOUR MONITORING



EMAIL

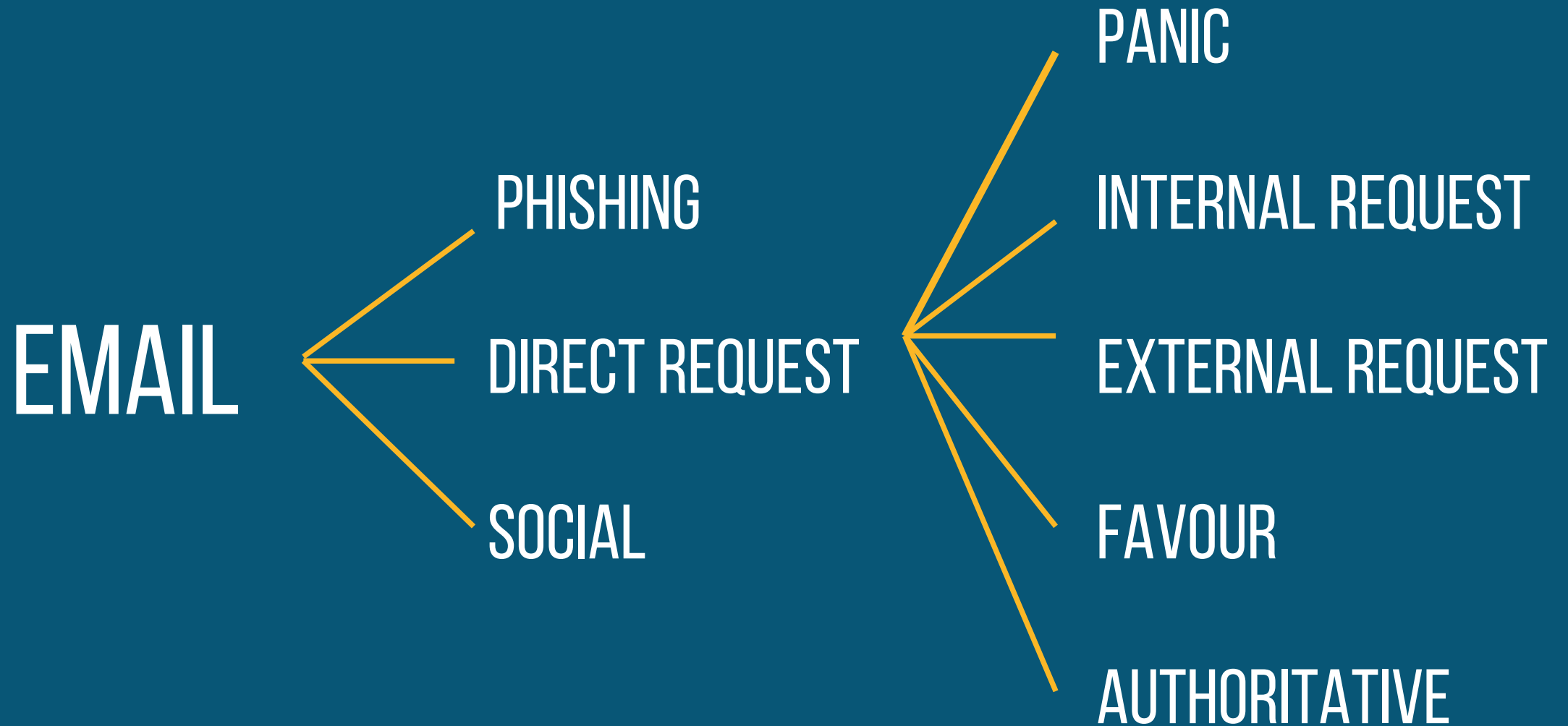
SOCIAL NETWORKS

REMOVABLE MEDIA

FILES AND HONEYPOTS

SMS

ATTACK VECTORS THAT MEAN SOMETHING



EMAIL ATTACKS THAT GO **BEYOND** PHISHING

The URL may be different on different messages.
Subject: Security Alert: Update Java (*See Kronos Note)
Date: February 22, 2013

USER GENERATED AND PUBLICLY SOURCED ATTACKS

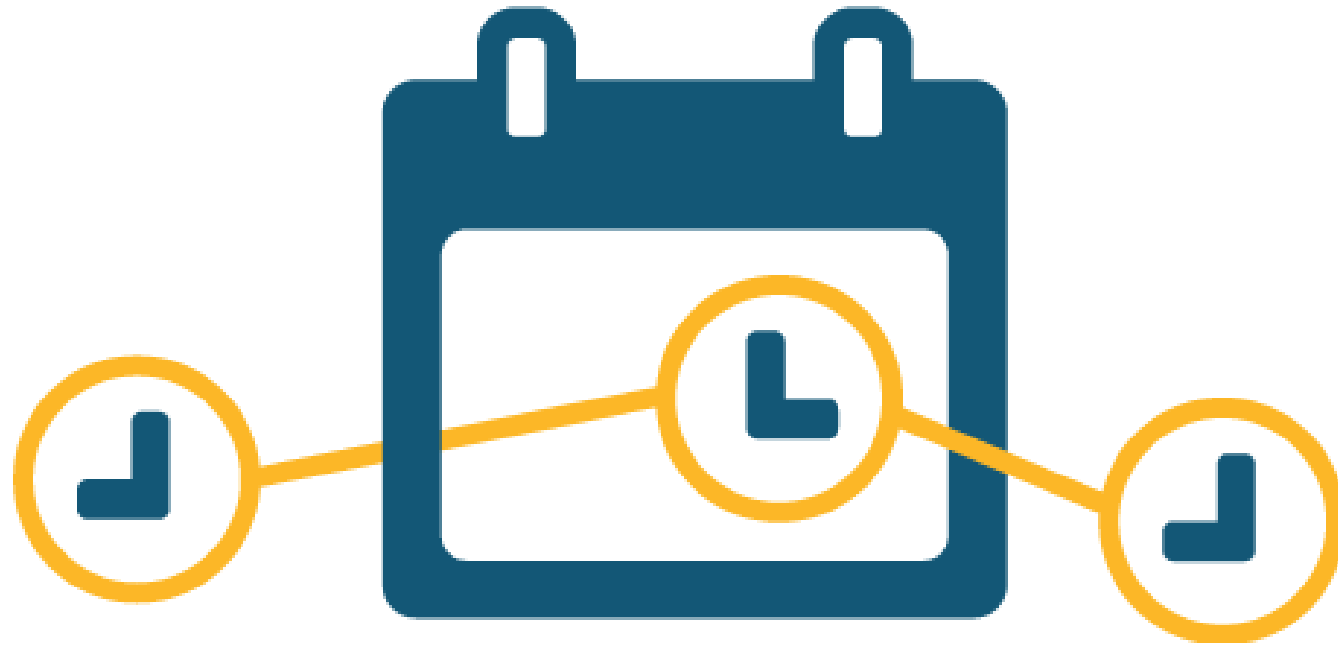
If you require assistance, please contact the Help Center.

Oracle has released an update for Java that fixes 50 security holes, including a critical hole currently being exploited in the wild.
The IT Security Office strongly recommends that you update Java as



REMOVING THE **BOUNDARIES** BETWEEN BUSINESS AND PERSONAL

SECURITY **FAILS** WHEN IT IS TREATED LIKE A SPECIAL EVENT



INSTANT, SCHEDULED AND RECURRING

GIVE THE OPTION OF SUCCEEDING
AND REINFORCE GOOD BEHAVIOURS

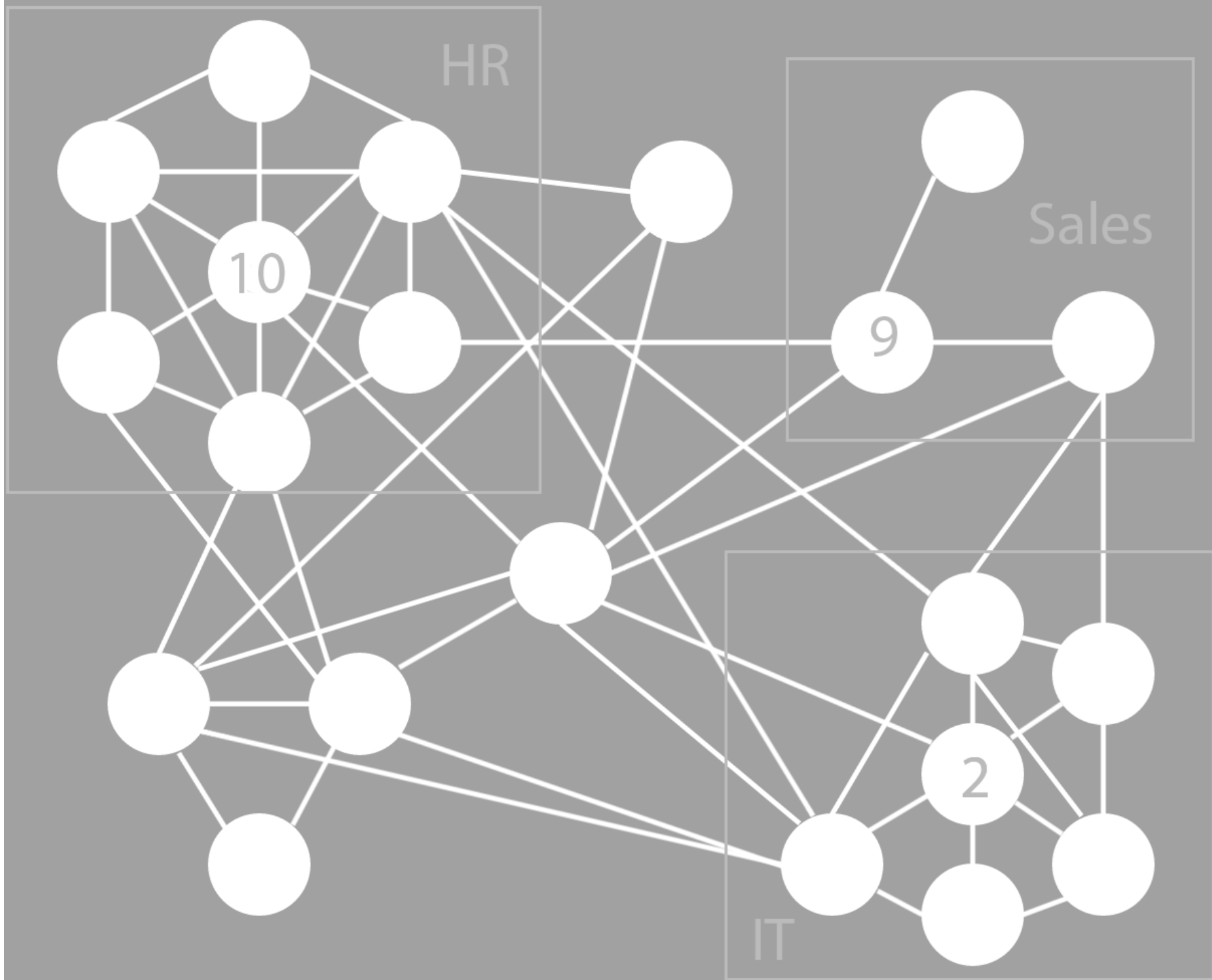


PHASE 3
ANALYSE

BEHAVIOUR VS. TIME



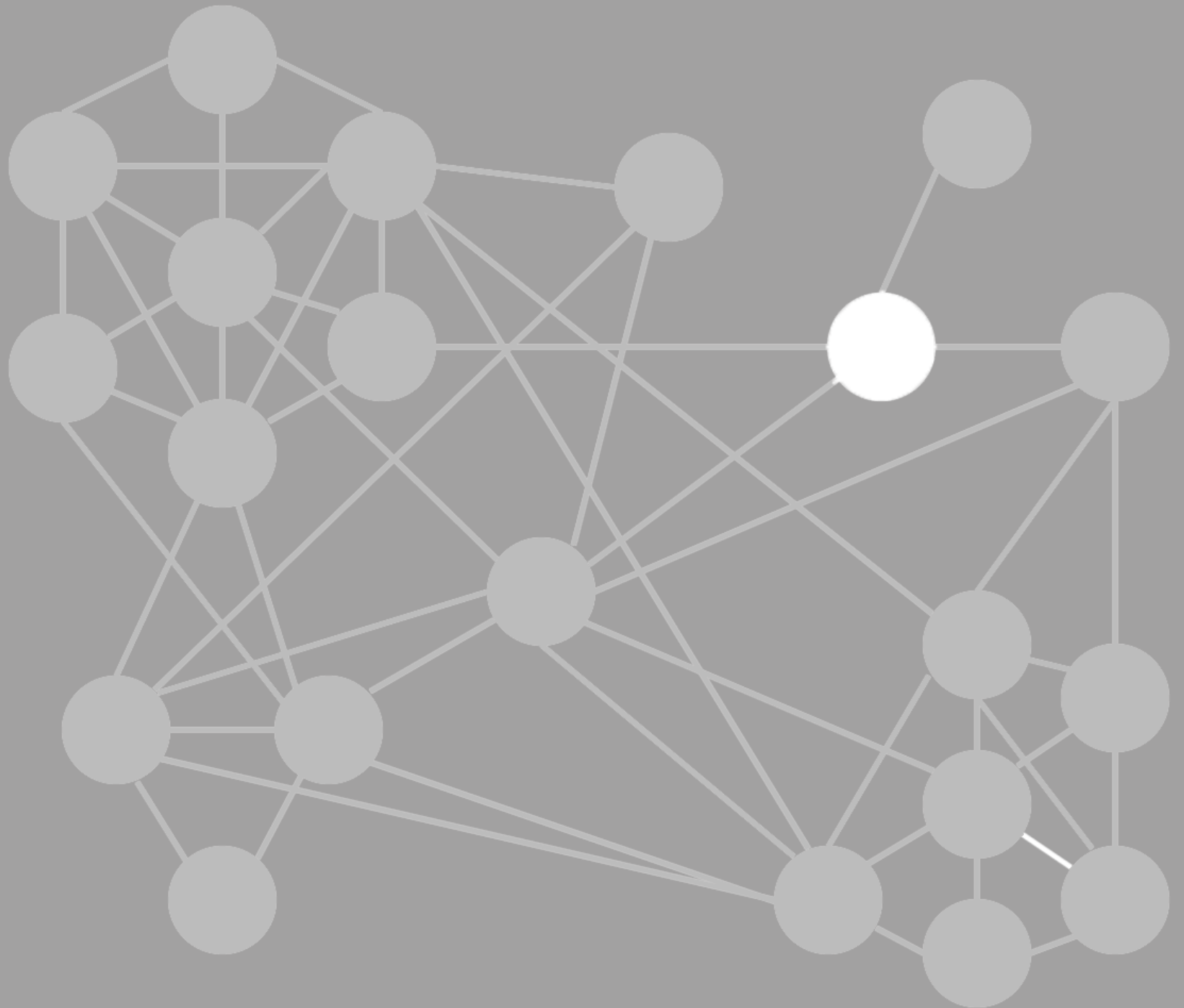
MEASURING IMPACT OF TRAINING



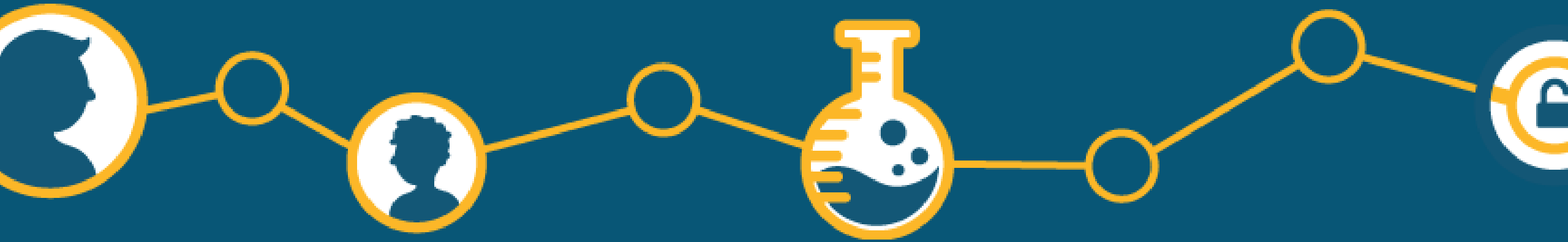
The background of the slide features a network diagram. It consists of several white circular nodes of varying sizes connected by thin white lines. The nodes are arranged in a way that suggests a complex web of relationships. A central node is particularly prominent, with many lines radiating from it. The overall aesthetic is clean and modern, with a focus on connectivity and structure.

BRIDGES, **WEAK LINKS** AND TARGETING

PIVOTING AND PROPAGATION



YOU KNOW WHAT WOULD BE FUN?



PREDICTIVE RISK BEHAVIOUR ANALYSIS

TECHNOLOGIES

- DJANGO
- POSTGRES SQL
- CELERY
- REDIS
- BOOTSTRAP
- OPEN SOURCE
- GPL
- VAGRANT + ANSIBLE BUILD
- INTEGRATES WITH EXCHANGE, AD AND GMAIL



PROTECT YOUR PEOPLE

But what is the cost of this dehumanisation? Should we be assessing human risk in a mechanical way? Is this progress or the slippery slope to a dystopian nightmare? Are we ready to harden up and remove emotion from the equation?

CAN WE AFFORD NOT TO?



QUESTIONS?



LAURA BELL

FOUNDER AND LEAD CONSULTANT - SAFESTACK

@lady_nerd , laura@safestack.io

<http://safestack.io>